STATEWIDE INFORMATION SYSTEMS POLICY

Statewide Policy: Internet/Intranet Security

Product ID: ENT-SEC-012

Effective Date: June 27, 2005

Approved: Janet R. Kelly, Director, Department of Administration

Replaces & Supercedes: This policy supercedes any prior enterprise policies for establishing and implementing information technology (IT) policies and standards.

I. Authorizations, Roles, & Responsibilities

Pursuant to the Montana Information Technology Act ("MITA") (Title 2, Chapter 17, Part 5 of the Montana Code Annotated ("MCA"), it is the policy of the state that information technology be used to improve the quality of life of Montana citizens, and that such improvement is to be realized by protecting individual privacy and the privacy of the information contained within the state's information technology systems. §2-17-505(1), MCA. It is also the policy of the state that the development of information technology resources be conducted in an organized, deliberative, and cost-effective manner, which necessitates the development of statewide information technology policies, standards, procedures, and guidelines applicable to all state agencies and others using the state network. It is also anticipated that State information technology systems will be developed in cooperation with the federal government and local governments with the objective of providing seamless access to information and services to the greatest degree possible. §2-17-505(2), MCA.

Department of Administration: Under MITA, the Department of Administration ("DOA") is responsible for carrying out the planning and program responsibilities for information technology for state government (except the national guard), including for establishing and enforcing a state strategic information technology plan and establishing and enforcing statewide information technology policies and standards. DOA is responsible for implementing MITA and all other laws for the use of information technology in state government. The director of DOA has appointed the chief information officer to assist in carrying out the department's information technology duties. §2-17-512, MCA.

Department Heads: Each department head is responsible for ensuring an adequate level of security for all data within their department. §2-15-114, MCA.

II. Policy - Requirements

A. Scope

This policy applies to all computers that reside on the state's network, including all state agencies as well as local government entities. This policy does not apply to colleges and universities, or the Commissioner of Higher Education Office.

B. Purpose

The Department of Administration's Information Technology Services Division (ITSD) is responsible for providing security for the Montana state network. This policy identifies the Internet/Intranet security responsibilities for both ITSD and entities that maintain computers on the state's network.

C. Requirements

The State of Montana network is a network shared by state agencies and local government entities that incorporates security measures to protect the State of Montana's information technology resources from outside entities. There are no expectations of privacy when using state computing resources unless explicitly indicated by law.

1. ITSD Internet/Intranet Security Responsibilities

ITSD will provide the following:

1. A separate area on the network referred to as the DMZ (Demilitarized Zone) for Internet Web and FTP Servers. All Internet web and ftp servers must reside on this area of the network. ITSD will also provide web and ftp hosting services for agencies that do not have the capabilities of moving servers to this isolated area on the network. ITSD can also house these servers in its secured data center.

2. Access from the trusted side of the state network to the Internet. Though typically unrestricted, some restrictions may be added at the discretion of ITSD if certain protocols or traffic is determined to be a security threat. ITSD will work with the Computer Security Incident Response Team to identify such security threats and determine the appropriate action. Some filters may be applied according to the Internet Filtering policy (ENT-SEC-121)

3. A firewall allowing only approved externally initiated access from the Internet to the trusted side of the state network. All requests for access through the firewall will be submitted to and reviewed by ITSD, who will approve or deny the requests. Such decisions may be appealed to the State Chief Information Officer.

4. A firewall between an agency or portion of an agency's network and the trusted state network will be provided at the agency's expense if requested. Agency firewalls will be installed and administered by ITSD unless precluded by statutory requirements.

5. Monitoring of all external connections to the trusted side of the state network. All external dial-up and dedicated connections must use the approved method as designated in policy ENT-SEC-130 Remote Access for Employees and Contractors.

6. Auditing of the state network including the detection and reporting of intrusion attempts performed continuously in an automated fashion. Daily review of the audit logs during the workweek. Agencies will be notified within 24 hours when their portion of the network is involved in any breaches of network security.

7. Management of Domain Name Services (DNS) and Internet Protocol (IP) Addresses. ITSD will assign IP addresses for authorized users of the state network. Agencies will use a private addressing scheme to provide additional security for network devices. All agencies will use the enterprise Domain Name Services (DNS) and Dynamic Host Configuration Protocol (DHCP) services.

8. Management and installation of all routers, switches, firewalls, hubs, access points and any new or future telecommunications devices that support the State of Montana network.

9. ITSD will conduct an annual security review of all agencies that have been granted exceptions to this policy.

ITSD may implement additional security measures as needed using software and/or hardware configurations for protecting the state network or ensuring secure communications. These may include encryption or filters restricting certain types of network traffic. All wireless connections to the inside (protected) portion of the network (inside) will be encrypted and authenticated. Unauthorized connections to the state network will not be permitted. Connections creating routing patterns that flood the network with unnecessary traffic are not allowed.

2. Agency Internet/Intranet Security Responsibilities

ITSD will take reasonable steps to make the state network as secure as possible, but agencies also have the responsibility for ensuring an adequate level of security for all data within their department.

Agencies will cooperate to make shared sites secure and may incorporate encryption into data transmission between sites on the wide area network (WAN).

Standard security checks must be made on Web Servers before they are made accessible to the public.

In accordance with the Remote Access Policy (ENT-SEC-130), an agency may allow remote access to its computing resources on a case-by-case basis. Approval for this access must be granted in writing by the appropriate agency management. Access will be granted for the benefit of the State of Montana and

not for personal benefit or use. Access to state computer resources by unauthorized remote access users shall be considered a security violation. Remote access users are obligated to abide by all computing policies of the state and the agency.

Security breaches, or suspicion of security breaches, must be reported to ITSD at the ITSD Service Desk.

D. Background - History On The Creation Of Or Changes To This Policy

The Department of Administration's Information Technology Services Division Network Security Officer created this policy. Included are issues addressed in a prior policy entitled "Access of State Computer Systems by Employees, Agents, or Contractors via Asynchronous Communications" which was replaced by this policy. The 2002 changes to the policy were proposed by the State Information Security Section and reviewed with the ITMC for comment prior to adoption.

Recommendations for modifications of this policy were made by the enterprise Security Committee in January 2005. The January 2005 modifications were discussed at two ITMC meetings and at a separate ITSD sponsored meeting on May 10, 2005.

E. Guidelines - Recommendations, Not Requirements

There are no guidelines for this policy.

F. Change Control and Exceptions

Policy changes or exceptions are governed by the Procedure for Establishing and Implementing Statewide Information Technology Policies and Standards. Requests for a review or change to this policy are made by submitting an Action Request form. Requests for exceptions are made by submitting an Exception Request form. Changes to policies and standards will be prioritized and acted upon based on impact and need.

III. Close

For questions or comments about this instrument, contact the Information Technology Services Division at ITSD Service Desk, or:

Chief Information Officer
PO Box 200113
Helena, MT 59620-0113
(406) 444-2700
FAX: (406) 444-2701

IV. Cross-Reference Guide

A. State/Federal Laws

- 2-17-505(1) – Policy
- 2-17-514(1) – Enforcement
- §2-17-505(2), MCA
- 2-17-512, MCA
- 2-17-534, MCA
- 2-15-114, MCA

B. State Policies (IT Policies, MOM Policies, ARM Policies)

- 2-15-112, MCA
- ARM 2.13.101 - 2.13.107 - Regulation of Communication Facilities
- MOM 3-0130 Discipline
- ARM 2.12.206 Establishing Policies, Standards, Procedures and Guidelines.

C. IT Procedures or Guidelines Supporting this Policy

- Policy: Establishing and Implementing Statewide Information Technology Policies and Standards
- Procedure: Establishing and Implementing Statewide Information Technology Policies and Standards

V. Administrative Use

Product ID:	ENT-SEC-012
Proponent:	Janet R. Kelly, Director, Department of Administration
Version:	1.1
Approved Date:	July 15, 2008
Effective Date:	June 27, 2005
Change & Review Contact:	ITSD Service Desk
Review Criteria:	Event Review: Any event affecting this policy may initiate a review. Such events may include a change in statute, key staff changes or a request for review or change.
Scheduled Review Date:	July 1, 2013
Last Review/Revision:	Reviewed July 11, 2008. Non-material changes are necessary.
Change Record:	July 11, 2008 – Non-material changes made: - Standardize instrument format and common components. - Changed to reflect next review date.